AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Previously Presented) A data transmitting system comprising a data recording medium and a drive unit which accesses the data recording medium,

the data recording medium including:

a security module which executes a mutual authentication protocol with the drive unit and a recording medium proper; and

the drive unit including:

a controller which executes the mutual authentication protocol when accessing the data recording medium; and

an interface unit which accesses the recording medium proper of the data recording medium;

wherein the data recording medium has self-identification data stored therein;

wherein the drive unit further includes a storage unit having self-identification data stored therein; and

wherein the security module of the data recording medium and controller of the drive unit exchange their own identification data between them to check whether their counterpart's own identification data is registered in an illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

2. (Original) The system as set forth in Claim 1, wherein the mutual authentication protocol uses the public-key encryption technology.

3. (Original) The system as set forth in Claim 1, wherein the data recording medium includes the security module and a disc as the data recording medium proper.

4. (Original) The system as set forth in Claim 3, wherein the drive unit further includes means for driving the disc as the recording medium proper of the data recording medium.

5. (Currently Amended) The system as set forth in Claim [[1]] 17, wherein the interface unit accesses directly the recording medium proper.

6. (Original) The system as set forth in Claim 1, wherein the data recording medium includes the security module and a memory chip as the recording medium proper.

7. (Original) The system as set forth in Claim 1, wherein the interface unit accesses the data recording medium via the security module of the data recording medium.

8. (Canceled)

9. (Previously Presented) The system as set forth in Claim 1, wherein the identification data of the data recording medium is stored in the security module.

10. (Previously Presented) The system as set forth in Claim 1, wherein the data recording medium has the list stored in the security module thereof.

11. (Previously Presented) The system as set forth in Claim 1, wherein the data recording medium has the list stored in the recording medium proper thereof.

12. (Previously Presented) The system as set forth in Claim 1, wherein the drive unit has the list stored in the storage unit thereof.

13. (Currently Amended) The system as set forth in Claim [[1]] 17, wherein the drive unit has not the list stored in the storage unit thereof.

14. (Currently Amended) The system as set forth in Claim [[1]] 17, wherein there is executed a mutual authentication protocol corresponding to whether either or both of the security module and drive unit itself holds the list or not.

15. (Currently Amended) The system as set forth in Claim [[1]] 17, wherein the controller of the drive unit judges whether or not the data recording medium is a one whose security module has the list stored therein, and executes a mutual authentication protocol which is based on the judgment result.

16. (Canceled)

17. (Currently Amended) The system as set forth in Claim 1, wherein:

the data recording medium stores ~~has stored~~ therein a first version of the illegal unit revocation list and a first ~~the~~ list version number ~~and the list itself~~;

the drive unit ~~has~~ stores therein a second version of the illegal unit revocation list and a second ~~the~~ list version number ~~and the list itself stored in the storage unit thereof~~; and

the ~~security module of the~~ data recording medium and ~~controller of~~ the drive unit exchange the first and second version numbers of ~~their own lists between them~~ when executing the mutual authentication protocol, and ~~one of them~~ whichever has a newer version of the illegal unit revocation list sends the newer version of the illegal unit

revocation list to the other while the other having an older version ~~list~~ updates its version list with the newer version ~~received new list~~.

18. (Previously Presented) The system as set forth in Claim 1, wherein:

the data recording medium has the list version number stored therein and the list itself recorded in the recording medium proper thereof;

the drive unit has the list version number and the list itself stored in the storage unit thereof;

the security module of the data recording medium and controller of the drive unit exchange the version numbers of their own revocation lists between them when executing the mutual authentication protocol; and

the drive unit will write the list to the data recording medium when the list stored in the storage unit of the drive unit is newer, while it will read the list from the data recording medium and update its own list with the list read from the data recording medium when its own list is older.

19. (Previously Presented) The system as set forth in Claim 1, wherein both the drive unit and security module check, using their own new lists, whether or not their counterpart's identification data are registered in the lists, respectively.

20. (Currently Amended) The system as set forth in Claim [[1]] 17, wherein:

the drive unit further includes a storage unit having self-identification data stored therein; and

the security module of the data recording medium receives the identification data from the drive unit and checks whether or not the identification data of the drive unit is registered in the illegal unit revocation list, when executing the mutual authentication

protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

21. (Currently Amended) The system as set forth in Claim [[1]] 17, wherein:

the data recording medium has self-identification data stored therein; and

the controller of the drive unit receives the identification data from the security module and checks whether or not the identification data of the security module is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

22. (Previously Presented) The system as set forth in Claim 1, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

23. (Previously Presented) The system as set forth in Claim 1, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

24. (Previously Presented) The system as set forth in Claim 1, wherein the illegal unit revocation list includes:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

25. (Currently Amended) The system as set forth in Claim 1, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is ~~a on having to be~~ considered revoked.

26. (Original) The system as set forth in Claim 1, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key from one of them to the other.

27. (Original) The system as set forth in Claim 1, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other.

28. (Original) The system as set forth in Claim 1, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the drive unit encrypts a data encrypting content key with a shared key obtained of the key sharing protocol and sends the encrypted data encrypting content key to the security module; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained of the key sharing protocol, re-encrypts the decrypted content key with a save key stored therein and sends the re-encrypted content key to the drive unit; and

the drive unit writes to the recording medium proper via the interface unit the data encrypted with the content key and the content key encrypted by the security module using the save key.

29. (Original) The system as set forth in Claim 1, wherein:

the drive unit is to read data from the recording medium proper via the interface unit;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the drive unit reads the encrypted content key from the recording medium proper and sends the read content key to the security module;

the security module decrypts the encrypted content key received from the drive unit with the save key stored therein, re-encrypts the decrypted content key with the shared key obtained of the key sharing protocol and sends the re-encrypted content key to the drive unit; and

the drive unit decrypts the encrypted content key received from the security module with the shared key obtained of the key sharing protocol, reads the content key-encrypted data from the recording medium proper and decrypts the read data.

30. (Original) The system as set forth in Claim 1, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the drive unit sends to the security module a data encrypting content key and having been encrypted with a shared key obtained of the key sharing protocol and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol and records to the recording medium proper the content key re-encrypted with a save key stored in the security module and data encrypted with the content key received from the drive unit.

31. (Original) The system as set forth in Claim 1, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the drive unit encrypts data with a shared key obtained through the execution of the key sharing protocol and sends the data thus encrypted to the security module; and

the security module decrypts the encrypted data received from the drive unit with the shared key, encrypts the decrypted data and stores the encrypted data into the recording medium proper.

32. (Original) The system as set forth in Claim 1, wherein:

the drive unit is to read data from the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the security module reads from the recording medium proper an encrypted content key and data encrypted with the content key, decrypts the encrypted content key with a save key stored therein and sends to the drive unit the content key re-encrypted with a shared key obtained through the execution of the key sharing protocol and data encrypted with the content key read from the recording medium proper; and

the drive unit decrypts the encrypted content key received from the security module with the shared key obtained through the execution of the key sharing protocol and decrypts the encrypted data with the content key.

33. (Original) The system as set forth in Claim 1, wherein:

the drive unit is to read data from the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the security module reads data encrypted and stored in the data recording medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data by the user of the shared key obtained through the execution of the key sharing protocol and sends the re-encrypted data to the drive unit; and the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted data received from the security module.

34. (Previously Presented) A data transmitting method for transferring data between a data recording medium having a recording medium proper and a drive unit which accesses the data recording medium, the method comprising steps of:

executing a mutual authentication protocol between a controller provided in the drive unit and a security module provided in the data recording medium; and

accessing, by the drive unit, the recording medium proper of the data recording medium according to the result of the mutual authentication protocol execution;

wherein the data recording medium has self-identification data stored therein;

wherein the drive unit further includes a storage unit having self-identification data stored therein; and

wherein the security module of the data recording medium and controller of the drive unit exchange their own identification data between them to check whether their counterpart's identification data is registered in an illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

35. (Original) The method as set forth in Claim 34, wherein the mutual authentication protocol is a protocol using the public-key encryption technology.

36. (Currently Amended) The method as set forth in Claim [[34]] 47, wherein the interface unit of the drive unit accesses directly the recording medium proper.

37. (Original) The method as set forth in Claim 34, wherein the interface unit of the drive unit accesses the data recording medium via the security module of the data recording medium.

38. (Canceled)

39. (Previously Presented) The method as set forth in Claim 34, wherein the data recording medium has the identification data stored in the security module thereof.

40. (Previously Presented) The method as set forth in Claim 34, wherein the data recording medium has the list stored in the security module thereof.

41. (Previously Presented) The method as set forth in Claim 34, wherein the data recording medium has the list stored in the recording medium proper thereof.

42. (Previously Presented) The method as set forth in Claim 34, wherein the drive unit has the list stored in the storage unit thereof.

43. (Currently Amended) The method as set forth in Claim [[34]] 47, wherein the drive unit has not the list stored in the storage unit thereof.

44. (Currently Amended) The method as set forth in Claim [[34]] 47, wherein there is executed a mutual authentication protocol corresponding to whether either or both of the drive unit and data recording medium holds the above list or not.

45. (Currently Amended) The method as set forth in Claim [[34]] 47, wherein the controller of the drive unit judges whether or not the data recording medium is a one whose security module has the list stored therein, and executes a mutual authentication protocol which is based on the judgment result.

46. (Canceled)

47. (Currently Amended) The method as set forth in Claim 34, wherein:

the data recording medium stores ~~has stored~~ therein a first version of the illegal unit revocation list and a first ~~the~~ list version number ~~and the list itself~~;

the ~~storage unit of the~~ drive unit stores therein a second version of the illegal unit revocation list and a second ~~stores the~~ list version number ~~and list itself therein~~; and

the ~~security module of the~~ data recording medium and ~~controller of~~ the drive unit exchange the first and second version numbers of ~~their own lists between them~~ when executing the mutual authentication protocol, and ~~one of them~~ whichever has a newer version of the illegal unit revocation list sends the newer version of the illegal unit revocation list to the other while the other having an older version ~~list~~ updates its version list with the newer version ~~received new list~~.

48. (Previously Presented) The method as set forth in Claim 34, wherein:

the data recording medium has the list version number stored therein and the list itself recorded in the recording medium proper thereof;

the drive unit has the list version number and list itself stored in the storage unit thereof;

the security module of the data recording medium and controller of the drive unit exchange the version numbers of their own revocation lists between them when executing the mutual authentication protocol; and

the drive unit writes the list to the data recording medium when the list stored in the storage unit thereof is a new one while the drive unit reads the list from the data recording medium and update its own list with the list read from the data recording medium when the list in the drive unit is an old one.

49. (Previously Presented) The method as set forth in Claim 34, wherein both the drive unit and security module check, using their own new lists, whether or not their counterpart's identification data are registered in the lists, respectively.

50. (Currently Amended) The method as set forth in Claim [[34]] 47, wherein:

the drive unit further includes a storage unit having self-identification data stored therein; and

the security module of the data recording medium receives the identification data from the drive unit and checks whether or not the identification data of the drive unit is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

51. (Currently Amended) The method as set forth in Claim [[34]] 47, wherein:

the data recording medium has self-identification data stored therein; and

the controller of the drive unit receives the identification data from the security module and checks whether or not the identification data of the security module is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

52. (Previously Presented) The method as set forth in Claim 34, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

53. (Previously Presented) The method as set forth in Claim 34, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

54. (Currently Amended) The method as set forth in Claim 34, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

55. (Currently Amended) The method as set forth in Claim 34, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is ~~included in the units having to be~~ considered revoked.

56. (Original) The method as set forth in Claim 34, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key from one of them to the other.

57. (Original) The method as set forth in Claim 34, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other.

58. (Original) The method as set forth in Claim 34, wherein:

the drive unit is to write data to the recording medium proper;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit encrypts the data content key with the shared key obtained through the execution of the key sharing protocol and sends the encrypted content key to the security module; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol, re-encrypts the content key decrypted with a save key stored therein and transmits the re-encrypted content key to the drive unit; and

the drive unit writes to the recording medium proper the data encrypted with the content key and the content key encrypted by the security module using the save key.

59. (Original) The method as set forth in Claim 34, wherein:

the drive unit is to read data from the recording medium proper;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit reads the encrypted content key from the recording medium proper and sends the read content key to the security module; and

the security module decrypts the encrypted content key received from the drive unit with the save key stored therein, re-encrypts the decrypted content key with the shared key obtained through the execution of the key sharing protocol and sends it to the drive unit; and

the drive unit decrypts the encrypted content key received from the security module with the shared key obtained through the execution of the key sharing protocol, reads the data encrypted with the content key from the recording medium proper and decrypts the read data.

60. (Original) The method as set forth in Claim 34, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit sends to the security module the data content key encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol and writes to the recording medium proper the content key re-encrypted with the save key stored in the security module and data encrypted with the content key received from the drive unit.

61. (Original) The method as set forth in Claim 34, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit encrypts data with the shared key obtained through the execution of the key sharing protocol and sends the data thus encrypted to the security module; and

the security module decrypts, with the shared key, the encrypted data received from the drive unit, encrypts the decrypted data and stores the encrypted data to the recording medium proper.

62. (Original) The method as set forth in Claim 34, wherein:

the drive unit is to read the encrypted data from the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the security module reads from the recording medium proper the encrypted content key and data encrypted with the content key, decrypts the encrypted content key with the save key stored therein and sends to the drive unit the content key re-encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key read from the recording medium proper; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted content key received from the security module and decrypts the encrypted data with the content key.

63. (Original) The method as set forth in Claim 34, wherein:

the drive unit is to read data from the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the security module reads data encrypted and stored in the data recording medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with the shared key obtained through the execution of the key sharing protocol and sends the re-encrypted data to the drive unit; and

the drive unit decrypts the encrypted data received from the security module with the shared key obtained through the execution of the key sharing protocol.

64. (Previously Presented) A drive unit which accesses a data recording medium including a recording medium proper and a security module which executes a mutual authentication protocol with the drive unit, the drive unit comprising:

a storage unit having self-identification data stored therein;

a controller which executes the mutual authentication protocol when accessing the data recording medium; and

an interface unit which accesses the recording medium proper of the data recording medium;

wherein when executing the mutual authentication protocol, the controller sends the identification data stored in the storage unit to the security module while receiving, from the security module, the self-identification data stored in the data recording

medium, to thereby check whether their counterpart's identification data are registered in respective illegal unit revocation lists, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a one having to be revoked.

65. (Original) The drive unit as set forth in Claim 64, wherein the mutual authentication protocol is a protocol using the public-key encryption technology.

66. (Original) The drive unit as set forth in Claim 64, further comprising a drive means for driving a disc as the recording medium proper of the data recording medium.

67. (Original) The drive unit as set forth in Claim 64, wherein the interface unit accesses a memory chip as the recording medium proper of the recording medium.

68. (Currently Amended) The drive unit as set forth in Claim [[64]] 75, wherein the interface unit accesses directly the recording medium proper.

69. (Original) The drive unit as set forth in Claim 64, wherein the interface unit accesses the recording medium proper of the data recording medium via the security module of the data recording medium.

70. (Canceled)

71. (Previously Presented) The drive unit as set forth in Claim 64, having the list stored in the storage unit thereof.

72. (Currently Amended) The drive unit as set forth in Claim [[64]] 75, having the list not stored in the storage unit thereof.

73. (Currently Amended) The drive unit as set forth in Claim [[64]] 75, wherein there is executed a mutual authentication protocol corresponding to whether either or both of the security module and drive unit itself holds the above respective lists or not.

74. (Canceled)

75. (Currently Amended) The drive unit as set forth in Claim 64, wherein:

the drive ~~storage~~ unit ~~thereof has stored the~~ stores therein a second version of the illegal unit revocation list and a second list version number ~~and the list itself~~; and

the ~~controller~~ drive unit transmits, when executing the mutual authentication protocol, the second list version number ~~stored in the storage unit~~ to the ~~security module~~ data recording medium while receiving, from the ~~security module~~ data recording medium, ~~the~~ a first list version number corresponding to a first version of the illegal unit revocation list that the data recording medium stores ~~holds~~ therein; and [[,]] ~~and sends, when~~

if the second version is newer than the first version ~~its list is a new one~~, the drive unit sends the second version ~~list~~ to the ~~security module~~ data recording medium; and

if the first version is newer than the second version, the drive unit updates the second version with the first version ~~while updating, when its list is an old one, the list with the new list~~ received from the ~~security module~~ data recording medium.

76. (Previously Presented) The drive unit as set forth in Claim 64, wherein:

the storage unit has stored therein the list version number and the list itself; and

the controller transmits, when executing the mutual authentication protocol, the list version number stored in the storage unit to the security module while receiving, from the security module, the list version number the data recording medium holds therein, and writes, when its list is a new one, the list to the recording medium proper of the data recording medium while reading, when its list is an old one, the list recorded in

the recording medium proper of the data recording medium, and updating its list with the read list.

77. (Previously Presented) The drive unit as set forth in Claim 64, adapted to work with the security module in checking, using their own new lists, whether or not their counterpart's identification data are registered in their own lists, respectively.

78. (Currently Amended) The drive unit as set forth in Claim [[64]] 75, wherein when executing the mutual authentication protocol, the controller receives, from the security module, the self-identification data held in the data recording medium, checks whether or not the identification data of the security module is registered in the illegal unit revocation list, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

79. (Previously Presented) The drive unit as set forth in Claim 64, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and the units registered in this list are taken as having to be revoked.

80. (Previously Presented) The drive unit as set forth in Claim 64, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

81. (Currently Amended) The drive unit as set forth in Claim 64, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

82. (Currently Amended) The drive unit as set forth in Claim 64, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is included in the listed units having to be revoked.

83. (Original) The drive unit as set forth in Claim 64, adapted to work with the security module, when executing the mutual authentication protocol, in executing a key sharing protocol using the public-key encryption technology, encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key from one of the drive unit and security module to the other.

84. (Original) The drive unit as set forth in Claim 64, adapted to work with the security module, when executing the mutual authentication protocol, in executing a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of the drive unit and security module to the other.

85. (Original) The drive unit as set forth in Claim 64, destined to write data to the recording medium proper via the interface unit, wherein:

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the data content key is encrypted with the shared key obtained through the execution of the key sharing protocol and the encrypted data content key is sent to the security module;

the security module decrypts the encrypted content key with the shared key obtained through the execution of the key sharing protocol, and receives data re-encrypted with the content key decrypted with save key stored therein; and

the data encrypted with the content key and the content key encrypted by the security module using the save key are recorded to the recording medium proper via the interface unit.

86. (Original) The drive unit as set forth in Claim 64, destined to read encrypted data from the recording medium proper via the interface unit, wherein:

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the encrypted content key is read from the recording medium proper and the read content key is sent to the security module; and

the security module decrypts the encrypted content key with the shared key obtained through the execution of the key sharing protocol and receives data re-encrypted with the content key decrypted with the shared key obtained through the execution of the key sharing protocol; and

the encrypted content key received from the security module is decrypted with the shared key obtained through the execution of the key sharing protocol, the data encrypted with the content key is read from the recording medium proper and decrypted.

87. (Original) The drive unit as set forth in Claim 64, destined to record data to the recording medium proper via the interface unit, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the data content key encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key are sent to the security module; and

the security module decrypts the encrypted content key with the shared key obtained through the execution of the key sharing protocol and writes to the recording medium proper the content key re-encrypted with the save key stored in the security module and data encrypted with the content key.

88. (Original) The drive unit as set forth in Claim 64, destined to write data to the recording medium proper via the interface unit, wherein

the interface unit accesses the recording medium proper via the security module of the data recording medium;

a protocol for key sharing with the security module is executed using the public-key encryption technology;

data is encrypted with the shared key obtained through the execution of the key sharing protocol and sent to the security module; and

the security module decrypts the encrypted data with the shared key, encrypts the decrypted data with the content key and stores the encrypted data to the recording medium proper.

89. (Original) The drive unit as set forth in Claim 64, destined to read data from the recording medium proper via the interface unit, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the security module reads from the recording medium proper the encrypted content key and data encrypted with the content key, decrypts the encrypted content key with the save key stored therein and receives the content key re-encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key read from the recording medium proper; and

the encrypted content key received from the security module is decrypted with the shared key obtained through the execution of the key sharing protocol and the encrypted data is decrypted with the content key.

90. (Original) The drive unit as set forth in Claim 64, destined to read data from the recording medium proper via the interface unit, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the security module reads data encrypted and stored in the data recording medium, decrypts the encrypted data with the content key, receives data resulted from re-encryption of the decrypted data with the shared key obtained through the execution of the key sharing protocol; and

the encrypted data received from the security module is decrypted with the shared key obtained through the execution of the key sharing protocol.

91. (Previously Presented) An access method for access to a data recording medium including a recording medium proper and a security module which executes a mutual authentication protocol with a drive unit, the method comprising steps of:

executing the mutual authentication protocol when accessing the data recording medium; and

accessing the recording medium proper of the data recording medium according to the result of the mutual authentication protocol execution;

wherein the drive unit stores self-identification data; and

wherein the drive unit and the security module of the data recording medium exchange, between them, the self-identification data stored in the drive unit and the identification data stored in the data recording medium, when executing the mutual authentication protocol, to check whether their counterpart's identification data is registered in an illegal unit revocation list, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

92. (Original) The method as set forth in Claim 91, wherein the mutual authentication protocol is a protocol using the public-key encryption technology.

93. (Original) The method as set forth in Claim 91, where access is made to a memory chip as the recording medium proper of the data recording medium.

94. (Currently Amended) The method as set forth in Claim [[91]] 99, wherein access is made directly to the recording medium proper.

95. (Original) The method as set forth in Claim 91, wherein the interface unit accesses the data recording medium via the security module of the data recording medium.

96. (Canceled)

97. (Currently Amended) The method as set forth in Claim [[91]] 99, wherein there is executed a mutual authentication protocol corresponding to whether either or both of the security module and drive unit itself holds the above list or not.

98. (Canceled)

99. (Currently Amended) The method as set forth in Claim 91, wherein:

the data recording medium stores ~~has stored~~ therein a first version of the illegal unit revocation list and a first ~~the~~ list version number; ~~and the list itself and~~

the drive unit ~~has~~ stores therein a second version of the illegal unit revocation list and a second ~~the~~ list version number ~~and the list itself stored in the storage unit thereof~~; and

the ~~security module of the~~ data recording medium and ~~controller of~~ the drive unit exchange the first and second version numbers of ~~their own lists between them~~ when executing the mutual authentication protocol, and ~~one of them~~ whichever has a newer

version of the illegal unit revocation list sends the newer version of the illegal unit revocation list to the other while the other having an older version ~~list~~ updates its version list with the newer version ~~received new list~~.

100. (Previously Presented) The method as set forth in Claim 91, wherein:

the data recording medium has the list version number stored therein and the list itself recorded in the recording medium proper thereof and the drive unit has the list version number and list itself stored in the storage unit thereof;

the security module of the data recording medium and controller of the drive unit exchange the version numbers of their own revocation lists between them when executing the mutual authentication protocol; and

the drive unit will write the list to the data recording medium when the list stored in the storage unit of the drive unit is a new one while the drive unit will read the list from the data recording medium and update its own list using the list read from the data recording medium when the list in the drive unit is an old one.

101. (Previously Presented) The method as set forth in Claim 91, wherein both the drive unit and security module check, using their own new lists, whether or not their counterpart's identification data are registered in the lists, respectively.

102. (Currently Amended) The method as set forth in Claim [[91]] 99, wherein:

the security module of the data recording medium receives the identification data from the drive unit and checks whether or not the identification data of the drive unit is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual

authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

103. (Previously Presented) The method as set forth in Claim 91, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

104. (Previously Presented) The method as set forth in Claim 91, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

105. (Currently Amended) The method as set forth in Claim 91, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

106. (Currently Amended) The method as set forth in Claim 91, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not the drive unit is included in the units having to be revoked.

107. (Original) The method as set forth in Claim 91, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt, using a shared key thus obtained, a data encrypting content key, and send the encrypted content key from one of them to the other.

108. (Original) The method as set forth in Claim 91, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other.

109. (Original) The method as set forth in Claim 91, wherein:

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit encrypts the data content key with the shared key obtained through the execution of the key sharing protocol and sends the encrypted data content key to the security module; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol, re-encrypts the content key decrypted with a save key stored therein and transmits the re-encrypted content key to the drive unit; and

the drive unit writes to the recording medium proper via the interface unit the data encrypted with the content key and the content key encrypted by the security module using the save key.

110. (Original) The method as set forth in Claim 91, wherein:

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit reads the encrypted content key from the recording medium proper and sends the read content key to the security module; and

the security module decrypts the encrypted content key with the save key stored in the security module, and receive data obtained by re-encrypting the

decrypted content key with the shared key obtained through the execution of the key sharing protocol; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted content key received from the security module, reads the data encrypted with the content key from the recording medium proper and decrypts the read data.

111. (Original) The method as set forth in Claim 91, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit sends to the security module the data content key encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol and writes to the recording medium proper the content key re-encrypted with the save key stored in the security module and data encrypted with the content key received from the drive unit.

112. (Original) The method as set forth in Claim 91, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium; the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit encrypts data with the shared key' obtained through the execution of the key sharing protocol and sends the data thus encrypted to the security module; and

the security module decrypts, with the shared key, the encrypted data received from the drive unit, encrypts the decrypted data and stores the encrypted data to the recording medium proper.

113. (Original) The method as set forth in Claim 91, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the security module reads from the recording medium proper the encrypted content key and data encrypted with the content key, decrypts the encrypted content key with the save key stored therein and sends to the drive unit the content key re-encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key read from the recording medium proper; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted content key received from the security module and decrypts the encrypted data with the content key.

114. (Original) The method as set forth in Claim 91, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the security module reads data encrypted and stored in the data recording medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with the shared key obtained through the execution of the key sharing protocol and sends the re-encrypted data to the drive unit; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted data received from the security module.

115. (Withdrawn) A data recording medium having a data recording area, comprising:

a security module having an interface function for interfacing with an external unit, a random number generating function, a data storing function, and a calculating function to provide a necessary calculation for mutual authentication protocol using the public-key encryption technology; and

a recording medium proper having the data recording area.

116. (Withdrawn) The data recording medium as set forth in Claim 115, wherein the security module further includes an interface function to access the data recording medium proper.

117. (Withdrawn) An access method for access to a data recording medium having a data recording area, the method comprising steps of:

connecting to an external unit;

generating a random number and sending it to the external unit;

making, using data received from the external unit and stored data, a necessary calculation for a protocol, for mutual authentication with the external unit, using the public-key encryption technology;

executing the mutual authentication mutual authentication protocol with the external unit; and

accessing a recording medium proper, in which data is to be recorded, of the data recording medium according to the result of the mutual authentication protocol execution.

118. (Withdrawn) A recording medium producing apparatus for producing a data recording medium, comprising:

a recording unit to record an illegal unit revocation list to the data recording medium which includes a recording medium proper in which data is to be recorded and a security module which executes a mutual authentication mutual authentication protocol with a drive unit which accesses the recording medium proper of the data recording medium.

119. (Withdrawn) The unit as set forth in Claim 118, further comprising an assembling unit to assemble the data recording medium including the security module and recording medium proper.

120. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records the list into the security module.

121. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records the list version number and the list itself into the security module.

122. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records the list in the recording medium proper.

123. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records the list version number into the security module and the list itself in the recording medium proper.

124. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit records, into the security module, the identification data of the data recording medium, private key and public key certificates which are to be used in the public key encryption technology given in the data recording medium, and the list version number.

125. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit further comprises means for storing the list which is to be recorded to the data recording medium.

126. (Withdrawn) The unit as set forth in Claim 118, wherein the recording unit further comprises an interface through which the list to be recorded into the data recording medium is acquired.

127. (Withdrawn) The unit as set forth in Claim 118, wherein the list is composed of a revocation list having registered therein identification data of units having to be revoked and/or a registration list having registered therein identification data of units having not to be revoked.

128. (Withdrawn) A recording medium producing method for producing a data recording medium, comprising a step of:

recording an illegal unit revocation list to the data recording medium which includes a recording medium proper in which data is to be recorded and a security module which executes a mutual authentication mutual authentication protocol with a drive unit which accesses the recording medium proper of the data recording medium.

129. (Withdrawn) The method as set forth in Clam 128, in which the data recording medium including the security module and recording medium proper is assembled.

130. (Withdrawn) The method as set forth in Claim 128, wherein the list is recorded into the security module.

131. (Withdrawn) The method as set forth in Claim 128, wherein the list version number and the list itself are recorded into the security module.

132. (Withdrawn) The method as set forth in Claim 128, wherein the list is recorded to the recording medium proper.

133. (Withdrawn) The method as set forth in Claim 128, wherein the list version number is recorded into the security module while the list itself is recorded to the recording medium proper.

134. (Withdrawn) The method as set forth in Claim 128, wherein the identification data of the data recording medium, private and public key certificates which are to be used in the public-key encryption technology given in the data recording medium, and the list are recorded into the security module.

135. (Withdrawn) The method as set forth in Claim 128, wherein the list is stored into the data recording medium.

136. (Withdrawn) The method as set forth in Claim 128, wherein the list to be recorded into the data recording medium is acquired from outside.

137. (Withdrawn) The method as set forth in Claim 128, wherein the list is composed of a revocation list having registered therein units having to be revoked and/or a registration list having registered therein units having not to be revoked.

138. (Previously Presented) The system as set forth in Claim 20, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

139. (Previously Presented) The system as set forth in claim 21, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

140. (Previously Presented) The system as set forth in Claim 20, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

141. (Previously Presented) The system as set forth in Claim 21, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

142. (Previously Presented) The system as set forth in Claim 20, wherein the illegal unit revocation list includes:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

143. (Previously Presented) The system as set forth in Claim 21, wherein the illegal unit revocation list includes:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

144. (Currently Amended) The system as set forth in Claim 20, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is ~~a on having to be~~ revoked.

145. (Currently Amended) The system as set forth in Claim 21, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is ~~a on having to be~~ revoked.

146. (Previously Presented) The method as set forth in Claim 50, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

147. (Previously Presented) The method as set forth in Claim 51, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

148. (Previously Presented) The method as set forth in Claim 50, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

149. (Previously Presented) The method as set forth in Claim 51, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

150. (Currently Amended) The method as set forth in Claim 50, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

151. (Currently Amended) The method as set forth in Claim 51, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

152. (Currently Amended) The method as set forth in Claim 50, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is included in the units having to be revoked.

153. (Currently Amended) The method as set forth in Claim 51, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is included in the units having to be revoked.

154. (Previously Presented) The drive unit as set forth in Claim 78, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and the units registered in this list are taken as having to be revoked.

155. (Previously Presented) The drive unit as set forth in Claim 78, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

156. (Currently Amended) The drive unit as set forth in Claim 78, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

157. (Currently Amended) The drive unit as set forth in Claim 78, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is included in the listed units having to be revoked.

158. (Previously Presented) The method as set forth in Claim 102, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

159. (Previously Presented) The method as set forth in Claim 102, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

160. (Currently Amended) The method as set forth in Claim 102, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

161. (Currently Amended) The method as set forth in Claim 102, wherein the illegal unit revocation list includes ~~consists of~~:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not the drive unit is included in the units having to be revoked.

162. (New) A storage apparatus for storing information retrieved by an information processing apparatus, the storage apparatus comprising:

a storage section for storing a first revoked unit list;

a receiving section for receiving a second revoked unit list from the information processing apparatus; and

a judging section for judging whether the information processing apparatus is revoked or not based on the first revoked unit list;

wherein if the information processing apparatus is revoked, the first revoked unit list is maintained, and if the information processing apparatus is not revoked, the first revoked unit list is replaced with the second revoked unit list.

163. (New) The storage apparatus as set forth in Claim 162, further comprising a receiving section for receiving ID information from the information processing apparatus.

164. (New) The storage apparatus as set forth in Claim 163, wherein the ID information includes a key for the information processing apparatus.

165. (New) The storage apparatus as set forth in Claim 164, wherein a digital certification includes the key.

166. (New) The storage apparatus as set forth in Claim 162, wherein the judging section judges whether the information processing apparatus is on the first revoked unit list.

167. (New) The storage apparatus as set forth in Claim 162, further comprising:

a comparing section for comparing the first revoked unit list with the second revoked unit list; and

a second judging section for judging which revoked unit list is newer.

168. (New) The storage apparatus as set forth in Claim 167, further comprising:

a transmitting section for transmitting the first revoked unit list to the information processing apparatus.

169. (New) The storage apparatus as set forth in Claim 167, wherein the second judging section compares the respective version information attached with each revoked unit list.

170. (New) The storage apparatus as set forth in Claim 162, further comprising:

a second receiving section for receiving a private key from the information processing apparatus;

a second storage section for storing a public key; and

a judging section for judging whether the private key and the public key correspond.

171. (New) The storage apparatus as set forth in Claim 170, wherein if the information processing apparatus is revoked or the private key does not relate to the public key, the first revoked unit list is maintained, and if the information processing apparatus is not revoked and the private key relates to the public key, the first revoked unit list is replaced with the second revoked unit list.

172. (New) The storage apparatus as set forth in Claim 171, wherein if the first revoked unit list is maintained and the information processing apparatus is not revoked, the first revoked unit list is transmitted to the information processing apparatus.

173. (New) The storage apparatus as set forth in Claim 162, wherein the storage section comprises:

a revoked unit list storage section for storing the first revoked unit list; and

a content storage section for storing content.

174. (New) The storage apparatus as set forth in Claim 173, wherein the revoked unit list storage section is more secure than the content storage section.

175. (New) The storage apparatus according to claim 162, wherein the first revoked unit list indicates at least one information processing apparatus whose private key has been revealed.

176. (New) The storage apparatus according to claim 162, wherein the storage apparatus and the information processing apparatus share a common private key.

177. (New) An information processing apparatus for retrieving information from a storage apparatus, comprising:

a storage section for storing a second revoked unit list;

a receiving section for receiving a first revoked unit list from the storage apparatus; and

a judging section for judging whether the storage apparatus is revoked or not based on the second revoked unit list;

wherein if the storage apparatus is revoked, the second revoked unit list is maintained, and if the storage apparatus is not revoked, the second revoked unit list is replaced with the first revoked unit list.

178. (New) The information processing apparatus as set forth in Claim 177, further comprising a receiving section for receiving ID information from the storage apparatus.

179. (New) The information processing apparatus as set forth in Claim 178, wherein the ID information includes a key for the storage apparatus.

180. (New) The information processing apparatus as set forth in Claim 179, wherein a digital certification includes the key.

181. (New) The information processing apparatus as set forth in Claim 177, wherein the judging section judges whether the storage apparatus is on the second revoked unit list.

182. (New) The information processing apparatus as set forth in Claim 177, further comprising:

a comparing section for comparing the first revoked unit list with the second revoked unit list; and

a second judging section for judging which revoked unit list is newer.

183. (New) The information processing apparatus as set forth in Claim 182, further comprising a transmitting section for transmitting the second revoked unit list to the storage apparatus.

184. (New) The information processing apparatus as set forth in Claim 182, wherein the second judging section compares the respective version information attached with each revoked unit list.

185. (New) The information processing apparatus as set forth in Claim 177, further comprising:

a second receiving section for receiving a private key from the storage apparatus;

a second storage section for storing a public key; and

a judging section for judging whether the private key and the public key correspond.

186. (New) The information processing apparatus as set forth in Claim 185, wherein if the storage apparatus is revoked or the private key does not relate to the public key, the second revoked unit list is maintained, and if the storage apparatus is not revoked and the private key relates to the public key, the second revoked unit list is replaced with the first revoked unit list.

187. (New) The information processing apparatus as set forth in Claim 186, wherein if the second revoked unit list is maintained and the storage apparatus is not revoked, the second revoked unit list is transmitted to the storage apparatus.

188. (New) The information processing apparatus as set forth in Claim 177, wherein the storage section comprises:

a revoked unit list storage section for storing the second revoked unit list; and

a content storage section for storing content.

189. (New) The information processing apparatus as set forth in Claim 188, wherein the revoked unit list storage section is more secure than the content storage section.

190. (New) The information processing apparatus as set forth in Claim 177, further comprising a playing back section for playing back information retrieved from the storage apparatus.

191. (New) The information processing apparatus according to claim 177, wherein the second revoked unit list indicates at least one storage apparatus whose private key has been revealed.

192. (New) The storage apparatus according to claim 177, wherein the storage apparatus and the information processing apparatus share a common private key.

193. (New) A system comprising an information processing apparatus and a storage apparatus, the information processing apparatus comprising:

a storage section for storing a second revoked unit list;

a receiving section for receiving a first revoked unit list from the storage apparatus; and

a judging section for judging whether the storage apparatus is revoked or not based on the second revoked unit list;

wherein if the storage apparatus is revoked, the second revoked unit list is maintained in the information processing apparatus, and if the storage apparatus is not revoked, the second revoked unit list is replaced with the first revoked unit list in the information processing apparatus; and

the storage apparatus comprising:

a storage section for storing the first revoked unit list;

a receiving section for receiving the second revoked unit list from the information processing apparatus; and

a judging section for judging whether the information processing apparatus is revoked or not based on the first revoked unit list;

wherein if the information processing apparatus is revoked, the first revoked unit list is maintained in the storage apparatus, and if the information processing apparatus is not revoked, the first revoked unit list is replaced with the second revoked unit list in the storage apparatus.

194. (New) The system as set forth in Claim 193, the information processing apparatus further comprising a receiving section for receiving ID information from the storage apparatus.

195. (New) The system as set forth in Claim 194, wherein the ID information is a key for the storage apparatus.

196. (New) The system as set forth in Claim 195, wherein a digital certification includes the key.

197. (New) The system as set forth in Claim 193, wherein the judging section for judging whether the storage apparatus is revoked judges whether the storage apparatus is on the second revoked unit list.

198. (New) The system as set forth in Claim 193, the information processing apparatus further comprising:

a comparing section for comparing the first revoked unit list with the second revoked unit list; and

a second judging section for judging which revoked unit list is newer.

199. (New) The system as set forth in Claim 198, the information processing apparatus further comprising a transmitting section for transmitting the second revoked unit list to the storage apparatus.

200. (New) The system as set forth in claim 198, wherein the second judging section compares the respective version information attached with each revoked unit list.

201. (New) The system as set forth in Claim 193, the information processing apparatus further comprising:

a second receiving section for receiving a private key from the storage apparatus;

a second storage section for storing a public key; and

a judging section for judging whether the private key and the public key correspond.

202. (New) The system as set forth in Claim 201, wherein if the storage apparatus is revoked or the private key does not relate to the public key, the second

revoked unit list is maintained, and if the storage apparatus is not revoked and the private key relates to the public key, the second revoked unit list is replaced with the first revoked unit list.

203. (New) The system as set forth in Claim 202, wherein if the second revoked unit list is maintained and the storage apparatus is not revoked, the second revoked unit list is transmitted to the storage apparatus.

204. (New) The system as set forth in Claim 193, wherein the storage section for storing the second revoked unit list comprises:

a revoked unit list storage section for storing the second revoked unit list; and

a content storage section for storing content.

205. (New) The system as set forth in Claim 204, wherein the revoked unit list storage section is more secure than the content storage section.

206. (New) The system set forth in Claim 193, the information processing apparatus further comprising a playing back section for playing back information retrieved from the storage apparatus.

207. (New) The system according to claim 193, wherein the second revoked unit list indicates at least one storage apparatus whose private key has been revealed.

208. (New) The system according to claim 193, wherein the storage apparatus and the information processing apparatus share a common private key.

209. (New) A method for retrieving information from a storage apparatus, comprising:

storing a second revoked unit list;

receiving a first revoked unit list from the storage apparatus; and

judging whether the storage apparatus is revoked or not based on the second revoked unit list;

wherein if the storage apparatus is revoked, the second revoked unit list is maintained, and if the storage apparatus is not revoked, the second revoked unit list is replaced with the first revoked unit list.

210. (New) The method as set forth in Claim 209, further comprising receiving ID information from the storage apparatus.

211. (New) The method as set forth in Claim 210, wherein the ID information includes a key for the storage apparatus.

212. (New) The method as set forth in Claim 211, wherein a digital certification includes the key.

213. (New) The method as set forth in Claim 209, wherein judging whether the storage apparatus is revoked includes judging whether the storage apparatus is on the second revoked unit list.

214. (New) The method as set forth in Claim 209, further comprising:

comparing the first revoked unit list with the second revoked unit list; and

judging which revoked unit list is newer.

215. (New) The method as set forth in Claim 214, further comprising transmitting the second revoked unit list to the storage apparatus.

216. (New) The method as set forth in claim 214, further comprising comparing the respective version information attached with each revoked unit list.

217. (New) The method as set forth in Claim 209, further comprising:

receiving a private key from the storage apparatus;

storing a public key; and

judging whether the private key and the public key correspond.

218. (New) The method as set forth in Claim 217, wherein if the storage apparatus is revoked or the private key does not relate to the public key, the second revoked unit list is maintained, and if the storage apparatus is not revoked and the private key relates to the public key, the second revoked unit list is replaced with the first revoked unit list.

219. (New) The method as set forth in Claim 218, wherein if the second revoked unit list is maintained and the storage apparatus is not revoked, the second revoked unit list is transmitted to the storage apparatus.

220. (New) The method as set forth in Claim 209, further comprising storing content.

221. (New) The method as set forth in Claim 220, wherein the revoked unit list is stored more securely than the content.

222. (New) The method set forth in Claim 209, further comprising playing back information retrieved from the storage apparatus.

223. (New) The method according to claim 209, wherein second revoked unit list indicates at least one storage apparatus whose private key has been revealed.

224. (New) The method according to claim 209, wherein the storage apparatus and the information processing apparatus share a common private key.